

English Translation of Relevant Portions of JP-A-2002-196983**Published on July 12, 2002**

:

:

Page (5), column 7, lines 26 -38

[0037] The demodulating means 201 demodulates a received digital broadcast signal. The error correcting means 202 corrects an error in the output of the demodulating means 201. The descrambling means 203 descrambles a signal that has been subjected to error correction. The separating means 204 separates the signal of a selected program from the descrambled signal, and outputs the separated signal. The encrypting means 205 encrypts the separated signal and outputs the encrypted signal. The encryption key generating means 207 generates an encryption key based on the identification data of the encryption key medium means 106, time, and the identification data of the receiver, and feeds the generated encryption key to the encrypting means 205. The authenticating means 206 authenticates the encryption key medium means 106, receives identification data, etc. of the encryption key medium means 106, encrypts the encryption key generated by the encryption key generating means 207, and transfers it to the encryption key medium means 106.

:

:

Page (5), column 7, line 48 –column 8, line 7

[0041] The authenticating means 301 authenticates the encryption key medium means 106, receives an encrypted encryption key, and releases the encryption to obtain the encryption key. The encryption releasing means 302 receives the encrypted signal of a selected program, and releases encryption using the encryption key received from the encryption key medium means 106. The decoding means 303 performs processing such as MPEG decoding on the decrypted signal. The image reproducing means 304 displays an image according to a decoded image signal. The sound reproducing means 305 reproduces sound according to a decoded audio signal, which is outputted via, for example, a speaker.

:

:

Page (6), column 9, line 30 – column 10, line 30

[0056] Fig. 8 is a block diagram showing the configuration of a first embodiment of the encryption key mediating unit according to the present invention. In this figure, as an example of the case where the receiver 101 and the presentation device 105 are connected to each other, a case is shown where an encryption key is mediated by a signal conductor through which the encrypted signal of a program is transmitted. The reference numeral 801 denotes encryption key to heat converting means, and the reference numeral 802 denotes thermal encryption key detecting means.

[0057] The encryption key to heat converting means 801 converts an encryption key generated by the encryption key generating means 207 into a temperature change, changing the temperature of the signal conductor. The thermal encryption key detecting means 802 detects the temperature change in the signal conductor, converts the temperature change into the encryption key, and feeds it to the encryption releasing means 302.

[0058] With this configuration, the encryption key is transmitted in the form of temperature change, and thus, if the coating of the cable is removed for the purpose of stealing the encryption key, the cable property changes, and thus the encryption key cannot be normally transmitted, which makes reproduction impossible; as a result, copyright can be protected.

[0059] Fig. 9 is a block diagram showing the configuration of a second embodiment of the encryption key mediating unit according to the present invention. In this figure, as an example of the case where the receiver 101 and the presentation device 105 are connected to each other, a case is shown where an encryption key is transmitted via a signal conductor through which the encrypted signal of a program is transmitted. The reference numeral 901 denotes encryption key to vibration converting means, and the reference numeral 902 denotes vibration encryption key detecting means.

[0060] The encryption key to vibration-converting means 901 converts the encryption key generated by the encryption key generating means 207 into data that is transmitted in the form of vibration, and this vibrates the signal conductor. The vibration encryption key detecting means 902 detects the data transmitted in the form of vibration, converts it into the encryption key, and

feeds it to the encryption releasing means 302.

[0061] With this configuration, the encryption key is transmitted in the form of vibration, and thus, if the cable is touched for the purpose of stealing the encryption key, the cable property changes, and the encryption key cannot be normally transmitted, which makes reproduction impossible; as a result, copyright can be protected.

[0062] Fig. 10 is a block diagram showing the configuration of a third embodiment of the encryption key mediating unit according to the present invention. In this figure, as an example of the case where the receiver 101 and the presentation device 105 are connected to each other, a case is shown where a superconductor is used as a signal conductor. The reference numeral 1001 denotes encryption key to magnetic field converting means, and the reference numeral 1002 denotes resistance encryption key detecting means.

[0063] The encryption key to magnetic field converting means 1001 converts the encryption key generated by the encryption key generating means 207 into a change of magnetic field strength, and applies it to the signal conductor. When the magnetic field is weak, the signal conductor remains superconductive and its resistance is zero. When the magnetic field is strong, the superconductivity of the signal conductor is destroyed and resistance appears therein. The resistance encryption key detecting means 1002 detects whether or not resistance has appeared, converts the detection result into the encryption key, and feeds it to the encryption releasing means 302.

[0064] With this configuration, the encryption key is transmitted in the form of resistance, and thus, if the cable is touched for the purpose of stealing the

encryption key, the cable property changes, and thus the encryption key cannot be normally transmitted, which makes reproduction impossible; as a result, copyright can be protected.

:

:

Page (7), column 11, line 48 – column 12, line 8

[0074] The authenticating section 1301 performs authentication between the device and the encryption key mediating unit. The volatile optical memory 1302 temporarily and optically stores the encryption key, with which the program has been encrypted, by use of a fluorescent substance or the like, and then automatically deletes it after a predetermined time has passed. The shutter section 1303 opens and closes a mechanical shutter or a liquid crystal shutter and the like when the encryption key is optically inputted or outputted. The light receiving section 1304 receives the optical pattern of the encryption key stored in the volatile optical memory 1302. The light emitting section 1305 emits light representing the encryption key in the form of an optical pattern. The encryption key converting section 1306 performs conversion between the encryption key and the optical pattern.

:

:

Page (8), column 13, line 21 – Page (9), column 15, line 21

[0088] Fig. 18 is a block diagram showing the configuration of another

embodiment of the encryption key mediating unit of the present invention. The reference numeral 1801 denotes an IC card, the reference numeral 1802 denotes IC card authenticating means, the reference numeral 1803 denotes encrypting/decrypting means, the reference numeral 1804 denotes device authenticating means, and the reference numeral 1805 denotes electromagnetic wave transmitting/receiving means.

[0089] The IC card 1801 stores an encryption key with which a program has been encrypted. The IC card authenticating means 1802 authenticates the IC card 1801, transfers the identification data of the IC card to the apparatus, and transfers an encryption key to the IC card. The encrypting/decrypting means 1803 decrypts an encrypted encryption key received from the apparatus, and then encrypts the decrypted encryption key to be in the state in which the encryption key is stored in the IC card 1801. The device authenticating means 1804 authenticates devices on a transmitting side and on a receiving side, and transmits and receives the encryption key. The electromagnetic wave transmitting/receiving means 1805, for example, uses an infrared ray to communicate with a receiver, and a radio wave to communicate with a presentation device. The electromagnetic wave transmitting/receiving means 1805 can operated such that, when the first and the second digital media devices are located in the vicinity, it uses an infrared ray to communicate with the two apparatuses, and when they are located far away, it uses an infrared ray to communicate with one of them and a radio wave to communicate with the other, or it uses a radio wave to communicate with both of them.

[0090] Thus, with this configuration, an IC card is installed, for example, in a

remote control unit, and thus the IC card can be moved from one device to the other in the remote control unit held in hand. Furthermore, a plurality of IC cards can be inserted into a single remote control unit to operate and authenticate each corresponding device, and thus copy right can be protected without forcing the user to perform an extra operation.

[0091] Fig. 19 is a block diagram showing the configuration of still another embodiment of the encryption key mediating unit. This configuration is obtained by adding device registering means 1901 to the configuration shown in Fig. 18.

[0092] The device registering means 1901 is for registering in advance a device to be used. The device authenticating means 1804 authenticates only a device that is registered in the device registering means 1901.

[0093] Thus, only a registered device is allowed to be used, and this prevents an unacceptable unauthorized device from being used; as a result, copy right can be protected.

[0094] Fig. 20 is a block diagram showing the configuration of still another embodiment of the encryption key mediating unit. The reference numeral 2001 denotes an encryption IC card, the reference numeral 2002 denotes encryption key decrypting means.

[0095] The encryption IC card 2001 encrypts an encryption key, with which a program has been encrypted, with an encryption key corresponding to the second digital media device, and stores the resulting encrypted encryption key. The IC card authenticating means 1802 authenticates the encryption IC card 2001, transfers the identification data of the encryption IC card to the device,

and transfers the encryption key to the IC card. The encryption key decrypting means 2002 decrypts the encrypted encryption key received from the device, and transfers it to the encryption IC card 2001 via the IC card authenticating means 1802. The device authenticating means 1804 authenticates the transmitting side and the receiving side devices, and transmits and receives an encryption key. The electromagnetic wave transmitting/receiving means 1805 uses, for example, an infrared ray to communicate with a receiver, and a radio wave to communicate with a presentation device.

[0096] Thus, a configuration can be achieved in which a remote control unit is used as an encryption key mediating unit corresponding to the transmitting side device, and in the remote control unit is installed an IC card that has an encryption function and corresponds to the second digital media device. This enables each of the first and the second digital media devices to transfer an encryption key using its unique code, and thus different device manufacturers can use different codes. This eliminates the need of publishing the encryption algorithm, making it easier to prevent leakage of the encryption key with which a program is encrypted.

[0097] Fig. 21 is a flow chart showing how a device is authenticated and an encryption key is transferred. Fig. 22 shows the process sequence among a receiver which is the first digital media device on the transmitting side, an encryption key mediating unit, and a presentation device which is the second digital media device on the transmitting side in the case where they are normally authenticated. The same numbers are given to processes that

correspond to those in Fig. 21. In Fig. 22, identification data is denoted by “ID” (hereinafter the same).

[0098] At step 2101, a program to be viewed is selected. At step 2102, an encryption key for encrypting the program is generated. At step 2103, authentication is performed between an encryption key mediating unit and the first digital media device on the transmitting side (e.g., a receiver, a reproducing device). At step 2104, the process branches according to whether or not the device is authenticated; when the device is not authenticated, the process is terminated. When the device is authenticated, the process proceeds to step 2105, where the encryption key is transferred to the encryption key mediating unit. At step 2106, the identification data of the encryption key mediating unit that has been transferred to the device on the transmitting side at the authentication is transferred from the first digital media device to the second digital media device on the receiving side (a presentation device, recording device, etc.). At step 2107, authentication is performed between the encryption key mediating unit and the second digital media device on the receiving side. At step 2108, the process branches according to the authentication result, and, when the device is not authenticated, the process is terminated. At step 2109, the encryption key is transferred from the encryption key mediating unit to the second digital media device on the receiving side.

[0099] As described above, the encryption key mediating unit is authenticated using its identification data that has been sent from the first digital media device on the transmitting side directly to the second digital media device on

the receiving side. As a result, even when an encrypted program data and an encryption key that is being transferred between the encryption key mediating unit and the device are drawn out and delivered, for example, via the Internet, the encryption key mediating unit cannot be authenticated at a recipient. This makes it impossible for the second digital media device on the receiving side to receive the encryption key, and thus illegal reproduction and viewing can be prevented.

:

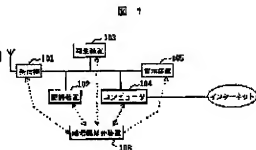
:

(11)Publication number : 2002-196983
(43)Date of publication of application : 12.07.2002

G06F 12/14
G06K 19/00
H04L 9/08
H04N 5/91
H04N 7/167

(71)Applicant : HITACHI LTD
(72)Inventor : AKIYAMA MORTYOSHI
SUGIYAMA YOSHIIICHI
TAKASHIMIZU SATOSHI
YONEDA SHIGERU
NEMOTO TOSHIYUKI
TSURUGA SADA O
KOREEDA HIROYUKI
OKAMURA TAKIIMI

SOLUTION: This transmitter for the encoded digital information and the cryptography key is provided with first digital media devices 101 and 103, the cryptography key medium device 106, and second digital media devices 105, 102, and 104. The first digital media devices encode the digital information by the cryptography key, output it to the second digital media devices as the encoded digital information, convert the cryptography key into a further encoded public key and output it to the cryptography key medium device. The second digital media devices decode the cryptography key from the public key inputted from the cryptography key medium device and decode the encoded digital information inputted from the first digital media devices by the cryptography key.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-196983

(P2002-196983A)

(43) 公開日 平成14年7月12日 (2002. 7. 12)

(51) Int.Cl. ⁷	識別記号	F I	データ [*] (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 K 19/00		G 0 6 K 19/00	Q 5 B 0 3 5
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A 5 C 0 5 3
H 0 4 N 5/91			6 0 1 E 5 C 0 6 4
7/167		H 0 4 N 5/91	P 5 J 1 0 4
審査請求 未請求 請求項の数14 O L (全 37 頁) 最終頁に続く			

(21) 出願番号 特願2000-396578 (P2000-396578)

(22) 出願日 平成12年12月27日 (2000. 12. 27)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 秋山 守慶

神奈川県横浜市戸塚区吉田町292番地 株

式会社日立製作所デジタルメディア開発本

部内

(72) 発明者 杉山 由一

神奈川県横浜市戸塚区吉田町292番地 株

式会社日立製作所デジタルメディア開発本

部内

(74) 代理人 100068504

弁理士 小川 勝男 (外2名)

最終頁に続く

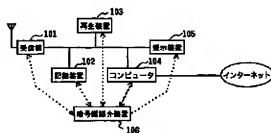
(54) 【発明の名称】 暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置

(57) 【要約】

【課題】著作権を保護しながら視聴者の使い勝手を考慮した新しい暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置を提供する。

【解決手段】第1のデジタルメディア機器 (101、103) と暗号鍵媒体装置 (106) と第2のデジタルメディア機器 (105、102、104) を備え、第1のデジタルメディア機器はデジタル情報を暗号鍵で暗号化して暗号化デジタル情報として第2のデジタルメディア機器に出力するとともに、暗号鍵をさらに暗号化した公開鍵にして暗号鍵媒体装置に出力し、第2のデジタルメディア機器は暗号鍵媒体装置から入力された公開鍵より暗号鍵を復号し、暗号鍵により第1のデジタルメディア機器から入力された暗号化デジタル情報を復号する。

図 1



【特許請求の範囲】

【請求項1】第1のデジタルメディア機器と、暗号鍵媒体装置と、第2のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、

前記第1のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化した暗号化デジタル情報として前記第2のデジタルメディア機器に出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記暗号鍵媒体装置に出力するように構成し、

前記暗号鍵媒体装置は、前記第1のデジタルメディア機器から入力された前記公開鍵より前記暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして前記第2のデジタルメディア機器に出力するように構成し、

前記第2のデジタルメディア機器は、前記暗号鍵媒体装置から入力された前記公開鍵より前記暗号鍵を復号し、前記暗号鍵により、前記第1のデジタルメディア機器から入力された前記暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置。

【請求項2】デジタル情報を暗号鍵で暗号化した暗号化デジタル情報として出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記出力とは別に出力するように構成したことを特徴とするデジタルメディア機器。

【請求項3】入力された公開鍵より前記公開鍵として暗号化された前の暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置。

【請求項4】入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号するように構成したことを特徴とするデジタルメディア機器。

【請求項5】請求項1記載の前記第1のデジタルメディア機器または請求項2記載の前記デジタルメディア機器がデジタル放送を受信する受信機であって、デジタル放送信号を復調し、誤りを訂正し、スクランブルを解除し、視聴を希望するデジタル情報を選択して分離し、選択されたデジタル情報を、前記暗号鍵で暗号化して出力するように構成したことを特徴とする受信機。

【請求項6】請求項1記載の前記第1のデジタルメディア機器または請求項2記載の前記デジタルメディア機器が再生装置であって、記録媒体からデジタル情報を再生し、前記暗号鍵で暗号化して出力するように構成したことを特徴とすることを特徴とする再生装置。

【請求項7】請求項1記載の前記第1のデジタルメディア機器または請求項4記載の前記デジタルメディア機器が提示装置であって、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号して表示するように構成したことを特徴とする提示装置。

【請求項8】請求項1記載の前記第1のデジタルメディア機器または請求項4記載の前記デジタルメディア機器が記録装置であって、入力された公開鍵より公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵をさらに暗号化した公開鍵にして、別に入力された暗号化デジタル情報とともに記録媒体に記録するように構成したことを特徴とする記録装置。

【請求項9】請求項1記載の前記第1のデジタルメディア機器または請求項4記載の前記デジタルメディア機器がコンピュータであって、入力された暗号化デジタル情報を記憶し、別に入力された暗号鍵は記憶しないか入力されないように構成したことを特徴とするコンピュータ。

【請求項10】請求項1または3記載の前記暗号鍵媒体装置は、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号して記憶手段に記憶するとともに、前記記憶手段に記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置。

【請求項11】第1のデジタルメディア機器と、暗号鍵媒体装置と、第2のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、前記第1のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化した暗号化デジタル情報として前記第2のデジタルメディア機器に出力し、前記暗号鍵媒体装置を認証してから生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成し、

前記暗号鍵媒体装置は、前記第1のデジタルメディア機器との認証時に前記暗号鍵媒体装置の識別情報を前記第1のデジタルメディア機器に転送し、前記第1のデジタルメディア機器から前記暗号鍵を入力するように構成し、

前記第2のデジタルメディア機器は、前記暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された前記暗号鍵により、前記第1のデジタルメディア機器から入力された、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置。

【請求項12】デジタル情報を暗号鍵で暗号化した暗号化デジタル情報として出力し、暗号鍵媒体装置を認証してから生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成したことを特徴とするデジタルメディア機器。

【請求項13】第1のデジタルメディア機器との認証時に識別情報を前記第1のデジタルメディア機器に転送し、前記第1のデジタルメディア機器から前記暗号鍵を入力するように構成したことを特徴とする暗号鍵媒体装置。

【請求項14】暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された暗号鍵により、別に入力さ

れた、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とするデジタルメディア機器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル放送等の送信側デジタルメディア機器から、DVDレコーダ、D-VHS VTRなどの受信側デジタルメディア機器に、暗号化デジタル情報を伝送する際の暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器なら

【0002】

【従来の技術】放送や、パッケージメディアがデジタル化され、劣化するこなしに複製を作ることが簡単にできるようになっている。このため、著作権保護のための機能が新たに必要とされるようになった。

【0003】特に課題となるのがパーソナルコンピュータである。記録できないようなストリーミングコンテンツについても、ディスプレイへのデジタル出力を違法に記録などの方法が考えられる。

【0004】それを防ぐ規格として、HDCP(High-bandwidth Digital Content Protection: White Paper →<http://www.siiimage.com/documents/SII-WP-002-A.pdf>)などが、提案されている。

【0005】これは、パソコンのディスプレイ出力を暗号化し、ディスプレイで復号するというもので、データとは別の線で、鍵交換を行い、認証された場合にのみ暗号化したデータを出力して、表示するというものであった。

【0006】

【発明が解決しようとする課題】しかしながら、パーソナルコンピュータ以外のA/V機器もデジタル化され、さらにそれらが相互に接続されたネットワークを構成するようになると、パソコンとディスプレイという限られた組み合わせ以外での著作権保護が必要となる。

【0007】また、コンピュータネットワークと、A/V機器のネットワークでは、規格が異なっていたが、IP over 1394など、A/V系のネットワークにコンピュータネットワークと共通のプロトコルを乗せる方法も開発されており、すべてのネットワークを1本の線で接続することも可能となってくる。

【0008】さらに、コンテンツ提供者の立場からは、コンテンツをインターネットなどに勝手に配信されることに対する不安から、著作権の保護方法が確立しないと、デジタル系のメディアに供給しにくいという課題もある。

【0009】本発明の目的は、著作権を保護しながら視聴者の使い勝手を考慮した新しい暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置を提供することにある。

【0010】

【課題を解決するための手段】本発明は、第1のデジタルメディア機器と、暗号鍵媒体装置と、第2のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、前記第1のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記暗号鍵媒体装置に出力するように構成し、前記暗号鍵媒体装置は、前記第1のデジタルメディア機器から入力された前記公開鍵より前記暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして前記第2のデジタルメディア機器に出力するように構成し、前記第2のデジタルメディア機器は、前記暗号鍵媒体装置から入力された前記公開鍵より前記暗号鍵を復号し、前記暗号鍵により、前記第1のデジタルメディア機器から入力された前記暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置である。

【0011】本発明は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、前記暗号鍵をさらに暗号化した公開鍵にして前記出力とは別に出力するように構成したことを特徴とするデジタルメディア機器である。

【0012】本発明は、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号して記憶し、前記記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置である。

【0013】本発明は、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号するように構成したことを特徴とするデジタルメディア機器である。

【0014】本発明で、前記第1のデジタルメディア機器または前記デジタルメディア機器がデジタル放送を受信する受信機であって、デジタル放送信号を復調し、誤りを訂正し、スクランブルを解除し、視聴を希望するデジタル情報を選択して分離し、選択されたデジタル情報を、前記暗号鍵で暗号化して出力するように構成したことを特徴とする受信機である。

【0015】本発明で、前記第1のデジタルメディア機器または前記デジタルメディア機器が再生装置であって、記録媒体からデジタル情報を再生し、前記暗号鍵で暗号化して出力するように構成したことを特徴とすることを特徴とする再生装置である。

【0016】本発明で、前記第1のデジタルメディア機器または前記デジタルメディア機器が提示装置であって、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵により、別に入力された暗号化デジタル情報を復号して表示するように構成

したことを特徴とする提示装置である。

【0017】本発明で、前記第1のデジタルメディア機器または請求項4記載の前記デジタルメディア機器が記録装置であって、入力された公開鍵より公開鍵として暗号化される前の暗号鍵を復号し、前記暗号鍵をさらに暗号化した公開鍵にして、別に入力された暗号化デジタル情報とともに記録媒体に記録するように構成したことを特徴とする記録装置である。

【0018】本発明で、前記第1のデジタルメディア機器または前記デジタルメディア機器がコンピュータであって、入力された暗号化デジタル情報を記憶し、別に入力された暗号鍵は記憶しないか入力されないように構成したことを特徴とするコンピュータである。

【0019】本発明で、入力された公開鍵より前記公開鍵として暗号化される前の暗号鍵を復号して記憶手段に記憶するとともに、前記記憶手段に記憶した前記暗号鍵を暗号化した公開鍵にして出力するように構成したことを特徴とする暗号鍵媒体装置である。

【0020】本発明は、第1のデジタルメディア機器と、暗号鍵媒体装置と、第2のデジタルメディア機器を備えた暗号化デジタル情報と暗号鍵の伝送装置であって、前記第1のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として前記第2のデジタルメディア機器に出力し、前記暗号鍵媒体装置を認証してから、生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成し、前記暗号鍵媒体装置は、前記第1のデジタルメディア機器との認証時に前記暗号鍵媒体装置の識別情報を前記第1のデジタルメディア機器に転送し、前記第1のデジタルメディア機器から前記暗号鍵を入力するように構成し、前記第2のデジタルメディア機器は、前記暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された前記暗号鍵により、前記第1のデジタルメディア機器から入力された、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とする暗号化デジタル情報と暗号鍵の伝送装置である。

【0021】本発明は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力し、暗号鍵媒体装置を認証してから生成した暗号鍵を前記暗号鍵媒体装置に出力するように構成したことを特徴とするデジタルメディア機器である。

【0022】本発明は、第1のデジタルメディア機器との認証時に識別情報を前記第1のデジタルメディア機器に転送し、前記第1のデジタルメディア機器から前記暗号鍵を入力するように構成したことを特徴とする暗号鍵媒体装置である。

【0023】本発明は、暗号鍵媒体装置を認証してから、前記暗号鍵媒体装置から入力された暗号鍵により、別に入力された、前記暗号鍵で暗号化された暗号化デジタル情報を復号するように構成したことを特徴とするデ

ジタルメディア機器である。

【0024】

【発明の実施の形態】図1は、本発明の実施の形態の構成のブロック図を示す。101は受信機、102はD-VHS VTRやDVDレコーダなどの記録装置、103はDVDプレーヤなどの再生装置、104はパーソナルコンピュータ（以下PCと略す）などのコンピュータ、105はディスプレイ、スピーカなどの提示装置、106は暗号鍵を媒介するためのケーブルやICカードその他の機器などの暗号鍵媒介装置である。

【0025】受信機101は、デジタル放送を受信しMPEGなどのフォーマットの信号に復号し、暗号化を施して出力する。記録装置102は、受信機101の出力する暗号化された信号を暗号化された状態でパッケージメディアに記録する。この時、暗号化に使用した暗号鍵は、暗号鍵媒介装置106を介して暗号化された状態で受け渡され、暗号化された状態で暗号鍵をパッケージメディアに記録する。また、記録装置102は、記録した暗号化された状態の信号をそのまま出力すると共に、暗号鍵媒介手段106を介して、暗号鍵を出力先に渡す。

【0026】再生装置103は、DVDなどのパッケージメディアを再生する。コンテンツ自体が暗号化されている場合は、それを解除した後に、再生装置103が暗号鍵を生成して暗号化を行い出力する。この際に生成した暗号鍵は暗号鍵媒介手段106を介して出力される。

【0027】コンピュータ104は、受信機101などから出力される信号を一時的に保管して出力する。暗号化された信号を記録して出力するが、暗号鍵は記録しないで、暗号鍵の識別情報のみを暗号鍵媒介手段106から受け取り記録する。

【0028】提示装置105は、暗号化された信号を入力し、暗号鍵媒介手段106から受け取った暗号鍵で暗号を解除した後、MPEGデコードなどの復号処理を行い、映像、音声を再生し提示する。また、提示装置105がディスプレイと複数のスピーカなどに分かれていて、暗号鍵媒介装置106がICカードなどの場合には、順々に、ICカードを装着し、すべての暗号鍵を転送しておく。

【0029】上記において、受信機101、再生装置103が本発明の第1のデジタルメディア機器に相当し、提示装置105、記録装置102、コンピュータ104が本発明の第2のデジタルメディア機器に相当する。

【0030】したがって、図1は、第1のデジタルメディア機器（受信機101、再生装置103）と、第2のデジタルメディア機器（提示装置105、記録装置102、コンピュータ104）と、暗号鍵媒体装置106の組み合わせから構成されている。

【0031】図1において、上記第1のデジタルメディア機器は、受信機101と再生装置103とが図示されているが、どちらか一方であって機器でもよい。また、

上記第2のデジタルメディア機器は、提示装置105と記録装置102とコンピュータ104とが図示されているが、少なくともひとつの機器であってもよい。

【0032】そして、第1のデジタルメディア機器は、デジタル情報を暗号鍵で暗号化して暗号化デジタル情報として出力するとともに、暗号鍵をさらに暗号化した公開鍵にして暗号鍵媒体装置106に出力する。

【0033】暗号鍵媒体装置108は、第1のデジタルメディア機器から入力された公開鍵より暗号鍵を復号して記憶するとともに、記憶した暗号鍵を暗号化した公開鍵にして第2のデジタルメディア機器に出力する。

【0034】第2のデジタルメディア機器は、暗号鍵媒体装置106から入力された公開鍵より暗号鍵を復号し、暗号鍵により、第1のデジタルメディア機器から入力された暗号化デジタル情報を復号する。

【0035】したがって、第1のデジタルメディア機器と第2のデジタルメディア機器との機器間では、暗号化されたデジタル信号が流れるため、違法にコピーしても再生することができず、著作権を保護することができる。

【0036】図2は、図1の受信機101の第1の実施の形態の構成のブロック図を示す。201は復調手段、202は誤り訂正手段、203はデスクランブル手段、204は分離手段、205は暗号化手段、206は認証手段、207は暗号鍵生成手段である。

【0037】復調手段201は、受信したデジタル放送信号を復調する。誤り訂正手段202は、復調手段201の出力の誤りを訂正する。デスクランブル手段203は、誤り訂正された後の信号にデスクランブル処理を行う。分離手段204は、デスクランブル済みの信号から選択した番組の信号を分離して出力する。暗号化手段205は、分離した信号に暗号化を施して出力する。暗号鍵生成手段207は、暗号鍵媒体装置106の識別情報や時刻、受信機の識別情報などを元にした暗号鍵を生成し、暗号化手段205へ出力する。認証手段206は、暗号鍵媒体装置106を認証し、識別情報などを受け取り、暗号鍵生成手段207の生成した暗号鍵を暗号化して暗号鍵媒体装置106へ転送する。

【0038】以上により、受信機で独自に暗号化を行って選択した番組の信号を出力し、暗号鍵は別系統で出力するために、違法コピーして再生することが困難である。

【0039】図3は、図1の提示装置105の第1の実施の形態の構成のブロック図を示す。

【0040】301は認証手段、302は暗号解除手段、303は復号手段、304は映像再生手段、305は音声再生手段である。

【0041】認証手段301は、暗号鍵媒体装置106を認証して、暗号化した暗号鍵を受け取り、暗号解除して暗号鍵を取り出す。暗号解除手段302は、選択した

番組の暗号化された信号を入力し暗号鍵媒体装置106から受け取った暗号鍵を用いて暗号を解除する。復号手段303は、暗号を解除された信号にMPEGデコードなどの処理を行う。映像再生手段304は、デコードされた映像信号をディスプレイ上に表示する。音声再生手段305は、デコードされた音声信号をスピーカなどで再生する。

【0042】以上により、正規に出力された信号のみ再生することができる。違法にコピーされた信号は再生することができなくなる。

【0043】図4は、図1の記録装置102の第1の実施の形態の構成のブロック図を示す。401は認証手段、402は暗号鍵用暗号鍵生成手段、403は暗号鍵暗号化復号化手段、404は記録手段である。

【0044】認証手段401は、暗号鍵媒体装置106を認証して、暗号化した暗号鍵を受け取り、暗号解除して暗号鍵を取り出して出力する。また、記録した番組を再生する場合には、暗号鍵を暗号化して暗号鍵媒体装置106へ転送する。暗号鍵用暗号鍵生成手段402は、認証手段401から暗号鍵媒体装置106の識別情報を受け取り、暗号鍵を暗号化するための暗号鍵を生成する。暗号鍵暗号化復号化手段403は、暗号鍵媒体装置106から受け取った暗号鍵に、暗号鍵用暗号鍵生成手段が生成した鍵で暗号化を行う。あるいは、暗号化された暗号鍵の暗号を解除して認証手段へ出力する。記録手段404は、選択した番組の暗号化された信号を記録するとともに、暗号鍵暗号化復号化手段403で暗号化された暗号鍵を記録する。

【0045】以上により、違法にコピーしたとしても、暗号鍵をさらに暗号化して記録しているために、再生することができない。

【0046】図5は、図1の再生装置103の第1の実施の形態の構成のブロック図を示す。501は認証手段、502は暗号鍵生成手段、503は暗号化手段、504は記録媒体である。

【0047】認証手段501は、暗号鍵媒体装置106を認証し、暗号鍵生成手段502の生成した暗号鍵を暗号化して暗号鍵媒体装置106へ転送する。暗号鍵生成手段502は、認証手段501から受け取った暗号鍵媒体装置106の識別情報などを元に暗号鍵を生成する。暗号化手段503は、記憶媒体504から出力するコンテンツの信号に暗号鍵生成手段502で生成した暗号鍵で、暗号化を施して出力する。記憶媒体504は、市販のDVDやD-VHSなどのパッケージメディアである。

【0048】以上により、パッケージメディアの再生時に、独自の暗号化を施して出力するため、違法コピーを防ぐことができる。

【0049】図6は、図1のコンピュータ103の第1の実施の形態の構成のブロック図を示す。

【0050】601は認証手段、602は演算手段、603は記憶装置、604は映像音声変換装置である。

【0051】認証手段601は、暗号鍵媒介装置106を認証し、暗号鍵の識別情報を受け取る。演算装置602は、認証手段から出力される暗号鍵の識別情報と、外部から入力した暗号化された番組の信号を入力し、記憶装置603へ記憶する。また、記憶装置603に記憶している番組の信号を外部へ出力すると同時に、暗号鍵の識別情報を認証手段601へ出力する。映像音声変換装置604は、コンピュータ内部で生成した映像、音声データを提示装置105で提示したり、記録手段102で記録する形式の信号に変換して出力する。

【0052】以上により、コンピュータ内部には、暗号化された信号のみを入力し、暗号鍵は入力されないため、インターネットなどに違法に配信しても、暗号鍵がないため再生できず、著作権を保護することができる。

【0053】図7は、図1の提示装置105の第2の実施の形態の構成のブロック図を示す。本構成では、図3の第1の実施の形態の構成に、入力先機器判定手段701と入力手段702が加えられている。

【0054】入力手段702は、各種機器の操作を入力する。入力先機器判定手段701は、入力手段702から入力した操作がどの機器に対するものかを判定して、その操作を対象とする機器へ転送する。

【0055】以上により、本構成例は、操作を提示手段に対してのみ行えばよいから、他の機器は、見えない場所に隠れていてもよい。このため、所有者以外の人間が機器を分解して内部の信号を盗むといったことを防ぐことも可能である。

【0056】図8は、暗号鍵媒介装置の第1の実施の形態の構成のブロック図を示す。この図では、受信機101と提示装置105を接続する場合の例で、暗号鍵の媒介に暗号化した番組を伝送する信号線を使用する場合を示している。801は暗号鍵熱変換手段、802は熱暗号鍵検出手段である。

【0057】暗号鍵熱変換手段801は、暗号鍵生成手段207で生成した暗号鍵を温度変化に変換して、信号線の温度を変化させる。熱暗号鍵検出手段802は、信号線の温度変化を検出し、暗号鍵へ変換して、暗号鍵解除手段302へ出力する。

【0058】本構成では、暗号鍵を温度変化として伝送するため、暗号鍵を盗もうとしてケーブルの被服を破ったりすると、特性が変わり正常に暗号鍵が伝送されずに再生することができなくなるため、著作権を保護することができる。

【0059】図9は、暗号鍵媒介装置の第2の実施の形態の構成のブロック図を示す。この図では、受信機101と提示装置105を接続する場合の例で、暗号鍵の媒介に暗号化した番組を伝送する信号線を使用する場合を示している。901は暗号鍵振動変換手段、902は振

動暗号鍵検出手段である。

【0060】暗号鍵振動変換手段901は、暗号鍵生成手段207で生成した暗号鍵を振動による伝達情報に変換して、信号線を振動させる。振動暗号鍵検出手段902は、信号線の振動による伝達情報を検出し、暗号鍵へ変換して、暗号鍵解除手段302へ出力する。

【0061】本構成では、暗号鍵を振動として伝送するため、暗号鍵を盗もうとしてケーブルに接触したりすると、特性が変わり正常に暗号鍵が伝送されずに再生することができなくなるため、著作権を保護することができる。

【0062】図10は、暗号鍵媒介装置の第3の実施の形態の構成のブロック図を示す。この図では、受信機101と提示装置105を接続する場合の例で、超伝導体を用いた信号線を使用する場合を示している。1001は暗号鍵境界変換手段、1002は抵抗暗号鍵検出手段である。

【0063】暗号鍵境界変換手段1001は、暗号鍵生成手段207で生成した暗号鍵を境界の強度変化に変換して、信号線に加える。境界が弱い場合は、信号線は超伝導状態を維持し電気抵抗が0になる。境界が強い場合には、超伝導を破壊して電気抵抗が表れる。抵抗暗号鍵検出手段1002は、信号線の抵抗のあるなしを検出し、暗号鍵へ変換して、暗号鍵解除手段302へ出力する。

【0064】本構成では、暗号鍵を抵抗として伝送するため、暗号鍵を盗もうとしてケーブルに接触したりすると、特性が変わり正常に暗号鍵が伝送されずに再生することができなくなるため、著作権を保護することができる。

【0065】図11は、暗号鍵媒介装置の第4の実施の形態の構成のブロック図を示す。1101は暗号鍵生成手段、1102は認証手段、1103は乱数発生手段、1104は記憶手段、1105は暗号化復号化手段である。

【0066】第1のデジタルメディア機器（受信機、再生装置など）に接続する場合、暗号鍵生成手段1101は、認証用の共通鍵と、番組を暗号化した暗号鍵を転送する際に使用する公開鍵とそれを復号する秘密鍵を生成する。乱数発生手段1103は、認証に使用する第2の乱数値を生成する。認証手段1102は、送信側機器から第1の乱数値を受け取り暗号鍵生成手段1101に第1の共通鍵を生成させ、暗号化復号化手段1105に第1の共通鍵で第2の乱数値を暗号化させて、暗号化した第2の乱数値を認証情報として、第2の乱数値とともに送信側機器に転送する。

【0067】第2の乱数値を元に生成した第2の共通鍵で、暗号鍵媒介手段106自身の識別情報を暗号化したものを送信側機器に転送する。暗号化復号化手段1105は、暗号鍵生成手段1101で生成した第1の共通鍵

で乱数発生手段1103が発生した乱数を暗号化し、第2の共通鍵で、暗号鍵媒介手段106の識別情報を暗号化する。また、暗号鍵生成手段1101で生成した公開鍵で暗号化された送信側機器から送られた暗号鍵を暗号鍵生成手段1101で生成した秘密鍵で復号する。記憶手段1104は、暗号化復号化手段1105で復号された暗号鍵を記憶する。

【0068】第2のデジタルメディア機器（提示装置、記録装置など）に接続する場合、暗号鍵生成手段1101は、受信側機器から転送された第3の乱数値を元に第3の共通鍵を生成する。暗号化復号化手段1105は、第3の共通鍵で暗号鍵媒介手段106の識別情報を暗号化して受信側機器へ転送する。また、受信側機器から転送された公開鍵で、記憶手段1104に記憶している暗号鍵を暗号化して出力する。認証手段1102は、受信側機器から第3の乱数値、公開鍵を受け取り、第3の共通鍵で暗号化した識別情報と、公開鍵で暗号化した暗号鍵を受信側機器へ転送する。

【0069】第2のデジタルメディア機器は、第1のデジタルメディア機器から転送された暗号鍵媒介手段の識別情報と、暗号鍵媒介手段から直接転送された識別情報が一致するかで認証を行うことにより、暗号鍵媒介装置から暗号鍵が盗まれても、暗号化した番組を再生できないようにすることができる。

【0070】図12は、図11の認証手段1102の構成のブロック図を示す。1201は提示手段、1202は認識手段、1203は交換手段、1204は処理部である。

【0071】提示手段1201は、暗号化した暗号鍵、公開鍵及び乱数値を2次元の光学パターンとして提示する。認識手段1202は、2次元の光学パターンを認識する。交換手段1203は、電気的な信号と光学パターンのデータとを交換する。処理部1204は、交換手段1203から出力される信号を入力し、認証処理を行う。暗号鍵媒介手段においては、暗号鍵生成手段1101、乱数発生手段1103、暗号化復号化手段1105に対して暗号鍵データや乱数値データを振り分けて処理を行わせる。

【0072】以上により、光学的に暗号鍵の受け渡しを行うため、短時間に大量の暗号鍵データを転送でき、待ち時間なしに操作を行うことができる。

【0073】図13は、暗号鍵媒介装置と第1のデジタルメディア機器、第2のデジタルメディア機器の認証手段の第1の実施の形態の構成のブロック図を示す。1301は認証部、1302は揮発性光学メモリ、1303はシャッター部、1304は受光部、1305は発光部、1306は暗号鍵交換部である。

【0074】認証部1301は、機器と暗号鍵媒介装置の間で認証処理を行う。揮発性光学メモリ1302は、番組を暗号化した暗号鍵を蛍光物質などで光学的に一時

的に記憶し、一定時間経過後には自動的に消去する。シャッター部1303は、暗号鍵を光学的に入力あるいは出力する際に機械的あるいは液晶などのシャッターを開閉する。受光部1304は、揮発性光学メモリ1302に記憶している暗号鍵の光学的パターンを受光する。発光部1305は、暗号鍵を光学的なパターンとして発光する。暗号鍵交換部1306は、暗号鍵と光学的パターンとの変換処理を行う。

【0075】以上により、暗号鍵媒介装置のシャッター部を強制的に開放すると光を受けて、暗号鍵が消去される、また、長時間放置していても揮発して消去されるために、暗号鍵を盗むことが困難になり、著作権を保護することができる。

【0076】図14は、暗号鍵媒介装置と第1のデジタルメディア機器、第2のデジタルメディア機器の認証手段の第2の実施の形態の構成のブロック図を示す。1401は記録部、1402は温度感応発生部、1403は暗号鍵交換部である。

【0077】認証部1301で認証処理を行い、認証された場合に番組を暗号化した暗号鍵の受け渡しを行う。記録部1401に暗号鍵を記録する。温度感応発生部は、暗号鍵を温度変化に変換して、機器の認証手段と暗号鍵媒介装置106の間で受け渡しを行う。暗号鍵交換部1403は、温度変化から暗号鍵へ変換する。

【0078】以上により、本構成では、暗号鍵を温度変化として受け渡すため、外部から盗むことが困難であり、著作権を保護することができる。

【0079】図15は、暗号鍵媒介装置と第1のデジタルメディア機器、第2のデジタルメディア機器の第3の実施の形態の構成のブロック図を示す。1501は圧力感応発生部、1502は暗号鍵交換部である。

【0080】認証部1301で認証処理を行い、認証された場合に番組を暗号化した暗号鍵の受け渡しを行う。記録部1401に暗号鍵を記録する。圧力感応発生部1501は、暗号鍵を圧力変化に変換して、機器の認証手段と暗号鍵媒介装置106の間で受け渡しを行う。暗号鍵交換部1502は、圧力変化から暗号鍵へ変換する。

【0081】以上により、本構成では、暗号鍵を圧力変化として受け渡すため、外部から盗むことが困難であり、著作権を保護することができる。

【0082】図16は、暗号鍵媒介装置と第1のデジタルメディア機器、第2のデジタルメディア機器の認証手段の第4実施の形態の構成のブロック図を示す。1601は超音波発生受信部、1602は暗号鍵交換部である。

【0083】認証部1301で認証処理を行い、認証された場合に番組を暗号化した暗号鍵の受け渡しを行う。記録部1401に暗号鍵を記録する。超音波発生受信部1601は、暗号鍵を超音波信号に変換して、機器の認証手段と暗号鍵媒介装置106の間で受け渡しを行う。

暗号鍵変換部1602は、超音波信号から暗号鍵へ変換す

【0084】以上により、本構成では、暗号鍵を超音波で受け渡すため、外部から盗むことが困難であり、著作権を保護することができる。

【0085】図17は、暗号鍵媒介装置の他の構成を示す図である。1701は可動導体、1702は接点である。

【0086】可動導体1701が第1のデジタルメディア機器にあり、第2のデジタルメディア機器の接点1702に接続することができる。暗号鍵は複数の可動導体1701を第2のデジタルメディア機器の接点1702に接続する、しないの組み合わせパターンと、可動導体1701の内部を伝送する信号の組み合わせによって伝送する。また、単純に可動導体を接続する接続しないという状態を用いるだけではなく、可動導体の先端部を複数の位置に移動するようにして、より複雑なパターンを伝送することも可能である。

【0087】以上により、暗号鍵の盗用が困難になり、著作権の保護ができる。

【0088】図18は、暗号鍵媒介装置の別の実施の形態の構成のブロック図を示す。1801はICカード、1802はICカード認証手段、1803は暗号化復号化手段、1804は機器認証手段、1805は電磁波送受信手段である。

【0089】ICカード1801は、番組を暗号化した暗号鍵を記憶する。ICカード認証手段1802は、ICカード1801を認証し、ICカードの識別情報を機器へ転送するとともに暗号鍵をICカードへ転送する。暗号化復号化手段1803は、機器から受け取った暗号化された暗号鍵を復号し、ICカード1801に保管する状態での暗号化を施す。機器認証手段1804は、送信側、受信側の機器を認証し、暗号鍵の送受信を行う。電磁波送受信手段1805は、機器とのやりとりを行う際に、例えば、受信機との間では赤外線を使用し、提示装置に対しては電波で通信するといったことを行う。第1のデジタルメディア機器と第2のデジタルメディア機器が近接した場所にある場合には、どちらも赤外線を使用して通信を行い、離れた場所にある場合には、片方は赤外線、もう一方を電波で通信する、あるいは、両方とも電波で通信を行うといった形態での使用が可能である。

【0090】以上により、本構成では、リモコンなどにICカードを装着して使用する形態となり、機器間でICカードなどを移動させる場合でも手元で行うことができる。また、複数のICカードを1台のリモコンに挿入して、各機器の操作および認証を行う構成なども可能となり、使用者に余分な操作を強いることなく著作権の保護ができる。

【0091】図19は、暗号鍵媒介装置のさらに別の実

施の形態の構成のブロック図を示す。図18の構成に、機器登録手段1901を追加した構成である。

【0092】機器登録手段1901は、使用する機器を事前に登録する。機器認証手段1804は、機器登録手段1901で登録されている機器に対しての認証を行う。

【0093】以上により、事前に登録した機器以外使用できないため、対応していない不正な機器は使用できなくなり、著作権を保護することができる。

【0094】図20は、暗号鍵媒介装置のさらに別の実施の形態の構成例のブロック図を示す。2001は暗号化ICカード、2002は暗号鍵復号化手段である。

【0095】暗号化ICカード2001は、番組を暗号化した暗号鍵を第2のデジタルメディア機器と対応する暗号鍵で暗号化して記憶する。ICカード認証手段1802は、暗号化ICカード2001を認証し、暗号化ICカードの識別情報を機器へ転送するとともに暗号鍵をICカードへ転送する。暗号鍵復号化手段2002は、機器から受け取った暗号化された暗号鍵を復号し、ICカード認証手段1802を介して、暗号化ICカード2001に転送する。機器認証手段1804は、送信側、受信側の機器を認証し、暗号鍵の送受信を行う。電磁波送受信手段1805は、機器とのやりとりを行う際に、例えば、受信機との間では赤外線を使用し、提示装置に対しては電波で通信するといったことを行う。

【0096】以上により、送信側の機器と対になった暗号鍵媒介装置としてリモコンを使用し、第2のデジタルメディア機器と対になった暗号化機能を備えたICカードをリモコンに装着する構成が可能となる。これにより、第1のデジタルメディア機器と第2のデジタルメディア機器それぞれが独自の暗号を使用した暗号鍵の転送を行うことができるため、機器の製造者ごとに異なる暗号を用いることができ、暗号アルゴリズムを公開する必要がなくなる。このため、番組を暗号化した暗号鍵の漏洩を防ぎやすくなる。

【0097】図21は、機器を認証して暗号鍵を転送する処理の流れ図を示す。また、図22は、正常に認証される場合の送信側の第1のデジタルメディア機器である受信機と暗号鍵媒介装置、送信側の第2のデジタルメディア機器である提示装置の間の処理シーケンスを示す。対応する処理に図21と同じ番号が付されている。ただし、図22では、識別情報をIDと記載してある（以下同様）。

【0098】ステップ2101は、視聴する番組を選択する。ステップ2102は、視聴する番組を暗号化する暗号鍵を生成する。ステップ2103は、暗号鍵媒介手段と送信側の第1のデジタルメディア機器（受信機、再生装置など）の間で認証を行う。ステップ2104は、認証処理の結果、正しい機器かどうかで処理を分岐し、認証されなかった場合には、処理を終了する。ステップ

2105は正しい機器だった場合で、暗号鍵媒体装置へ暗号鍵を転送する。ステップ2106は、認証時に送信側機器へ転送した暗号鍵媒体装置の識別情報を第1のデジタルメディア機器から受信側の第2のデジタルメディア機器（提示装置、記録装置など）へ転送する。ステップ2107は、暗号鍵媒体装置と受信側の第2のデジタルメディア機器の間での認証を行う。ステップ2108は、認証の結果が正しいかどうかで処理を分岐し、認証されなかった場合は処理を終了する。ステップ2109は、暗号鍵媒体装置から受信側の第2のデジタルメディア

機器へ暗号鍵を転送する。
 【0099】以上により、送信側の第1のデジタルメディア機器から直接受信側の第2のデジタルメディア機器に送られた暗号鍵媒体装置の識別情報を使って、暗号鍵媒体装置の認証を行うため、暗号化された番組データと、暗号鍵媒体装置と受け渡し中の暗号鍵を取り出してインターネットなどに配信したりしても、配信先では、暗号鍵媒体装置を認証することができない。このため、受信側の第2のデジタルメディア機器が暗号鍵を受け取ることができる、違法に再コピーして視聴することを防ぐことができる。

【0100】図23は、暗号鍵媒体装置と機器の認証処理だけの流れ図を示す。また、図24は、受信機と暗号鍵媒体装置、提示装置の間の処理シーケンスを示す。対応する処理に図22と同じ番号が付されている。

【0101】ステップ2301は、送信側機器が暗号鍵媒体装置へ時刻に応じた乱数値を転送する。ステップ2302は、送信側機器と暗号鍵媒体装置が乱数値を元に第1の共通鍵を生成する。ステップ2303は、暗号鍵媒体装置が第2の乱数値を生成し、第2の乱数値を第1の共通鍵で暗号化したものと共に送信側機器へ転送する。ステップ2304は、送信側機器が第2の乱数値と、第1の共通鍵で暗号化した第2の乱数値を復号化したものが、同一であることを確認する。ステップ2305は、第2の乱数値を元に、送信側機器と暗号鍵媒体装置が第2の共通鍵を生成する。ステップ2306は、第2の共通鍵で暗号鍵媒体装置の識別情報を暗号化して、送信側機器へ転送する。ステップ2307は、暗号鍵媒体装置の識別情報を第2の共通鍵で復号する。ステップ2308は、送信側機器が記録装置の場合には、記録している識別情報と一致するかを確認する。

【0102】ステップ2309は、受信側機器が公開鍵を送信側機器へ転送する。ステップ2410は、送信側機器が、受信側機器の公開鍵で、暗号鍵媒体装置の識別情報を暗号化する。ステップ2413は、暗号化した識別情報を受信側機器へ転送する。ステップ2414は、受信側機器が対応した秘密鍵を使って、暗号鍵媒体装置の識別情報を復号する。ステップ2415は、受信側機器が第3の乱数値を生成し暗号鍵媒体装置へ転送する。

【0103】ステップ2414は、暗号鍵媒体装置と受

信側機器が、第3の乱数値をもとに第3の暗号鍵を生成する。ステップ2415は、暗号鍵媒体装置が識別情報を第3の暗号鍵で暗号化して受信側機器へ転送する。ステップ2416は、受信側機器が識別情報を復号して、送信側機器から転送されたICカードの識別情報と一致することを確認する。ステップ2417は、受信側機器が記録装置の場合に、ICカードの識別情報を記録する。

【0104】以上により、送信側機器と受信側機器と、暗号鍵媒体装置の3者の間で認証が成立しない限り視聴することも、記録することもできないため、なんらかの方法で違法コピーしても再生することができず、著作権を保護することができる。

【0105】図25は、暗号鍵を送信側機器から受信側機器へ転送する処理だけの流れ図を示す。図26は、受信機と暗号鍵媒体装置、提示装置の間の処理シーケンスを示す。対応する処理に図23と同じ番号がふされている。

【0106】ステップ2501は、暗号鍵媒体装置が公開鍵を送信側機器へ転送する。ステップ2502は、送信側機器が番組を暗号化するのに使用した暗号鍵を、暗号鍵媒体装置の公開鍵で暗号化する。ステップ2503は、暗号化した暗号鍵を暗号鍵媒体装置へ転送する。ステップ2504は、暗号鍵媒体装置が対応した秘密鍵で暗号鍵を復号する。ステップ2505は、受信側機器の公開鍵を暗号鍵媒体装置へ転送する。ステップ2506は、暗号鍵媒体装置が、受信側機器の公開鍵で暗号鍵を暗号化する。ステップ2507は、暗号化した暗号鍵を受信側機器へ転送する。ステップ2508は、受信側機器が対応した秘密鍵で、暗号鍵を復号する。ステップ2509は、受信側機器が記録装置の場合には、暗号鍵を独自に暗号化して記録する。

【0107】以上により、認証された相手の公開鍵で暗号鍵を暗号化して渡すため、記録されない不正な機器には暗号鍵を転送しないため、著作権を保護できる。

【0108】図27は、暗号鍵媒体装置として、送信側機器と受信側機器を直接接続する形態をとる場合の認証と暗号鍵の転送処理の流れ図を示す。

【0109】ステップ2701は、送信側機器が公開鍵を受信側機器へ転送する。ステップ2702は、受信側機器が乱数値を発生し、受信側機器の識別情報と共に、送信側機器の公開鍵で暗号化して、送信側機器へ転送する。ステップ2703は、送信側機器が秘密鍵で、受信側機器の識別情報と乱数値を復号する。ステップ2704は、送信側機器と受信側機器が乱数値を元に共通鍵を生成する。この際に、送信側機器は、複数の受信側機器から送られた乱数値の中から、使用する受信側機器（提示装置のみ、提示装置と記録装置、記録装置のみなど）の乱数値を選択して共通鍵を生成する。

【0110】ステップ2705は、送信側機器が、暗号鍵と送信する受信側機器の識別情報を共通鍵で暗号化し

て、受信側機器へ転送する。ステップ2706は、受信側機器が自分宛てに送られてきた暗号鍵を、共通鍵で復号する。

【0111】以上により、複数の機器が接続された状態で、目的とする機器にのみ暗号鍵を転送することができ、他の機器で番組を再生したり、記録したりすることを防ぐことができる。

【0112】図28は、PCなどのコンピュータへ出力する場合の処理の流れ図を示す。

【0113】ステップ2801は、出力先にコンピュータを選択する。ステップ2802は、記録する番組を選択する。ステップ2803では、送信側機器が、選択した番組を暗号化する暗号鍵を生成する(記録装置の場合は、記録している暗号鍵の暗号を解除する)。ステップ2804では、暗号鍵媒介装置を認証する。ステップ2805では、認証結果が正しいかどうかで処理を分岐し、正しくない場合には終了する。

【0114】ステップ2806は、正しく認証した場合で、暗号鍵媒介装置へ暗号化した暗号鍵を転送する。ステップ2807は、暗号鍵媒介装置からコンピュータへ、暗号鍵の識別情報のみを転送する。ステップ2808は、コンピュータが、暗号鍵の識別情報と暗号化された番組を記録する。

【0115】以上により、コンピュータに記録する場合は、暗号鍵を記録しないため、インターネットへ配信して、視聴させるということができる。

【0116】図29は、PCなどのコンピュータが送信側機器になった場合に視聴する処理の流れ図を示す。

【0117】ステップ2901は、出力先の機器(提示装置、記録装置など)を選択する。ステップ2902は、視聴あるいは記録する番組を選択する。ステップ2903は、暗号鍵の識別情報を暗号鍵媒介装置へ転送する。ステップ2904は、出力先の機器の認証を行う。ステップ2905は、認証結果が正しいかどうかで処理を分岐し、正しくない場合には終了する。ステップ2906は、正しく認証された場合で、暗号鍵媒介装置から暗号鍵を出力先機器へ転送する。ステップ2907は、コンピュータから暗号化された番組を出力先へ転送する。

【0118】以上により、コンピュータ単体では、再生して視聴することができなくて、正規の提示装置と接続して初めて視聴できる。また、正規の提示装置に対してのみ記録させることが可能となり、違法な機器やネットワークに配信して利用させることを防ぐことができる。

【0119】図30、図31、図32は、記録に制限がある場合を含めた処理の流れ図を示す。

【0120】ステップ3001は、出力先の機器を選択する。ステップ3002は、視聴あるいは、記録する番組を選択する。ステップ3003は、出力先が提示装置かどうかを判定する。ステップ3004は、出力先が提

示装置で無い場合で、記録手段かどうかの判定処理へ分岐する。

【0121】ステップ3005は出力先が提示装置だった場合で、暗号鍵媒介装置の認証を行う。ステップ3006は、暗号鍵媒介装置へ暗号鍵と、複写属性情報を転送する。ステップ3007は、暗号鍵媒介装置と提示装置の間で認証を行う。ステップ3008は、暗号鍵媒介装置から提示装置へ暗号鍵を転送する。

【0122】ステップ3004へ分岐した後は、ステップ3009で、出力先が記録装置かどうか判定する。ステップ3010は、記録装置ではなかった場合で、出力先がコンピュータかどうかの判定処理へ分岐する。

【0123】ステップ3011は、出力先が記録装置であった場合で、選択した番組が複写を許可されているかどうかを判定し、許可されていない場合には処理を終了する。

【0124】ステップ3012は、複写が許可されていた場合で、この場合には、複写が1回のみの許可されているかどうかを判定する。ステップ3013は、1回のみ複写が許可されている場合で、暗号鍵媒介装置の認証を行う。

ステップ3014は、暗号鍵媒介装置から暗号鍵と、1回のみ複写可の複写属性情報を転送する。ステップ3015は、暗号鍵媒介装置と記録装置間で認証を行う。ステップ3016は、暗号鍵媒介装置から暗号鍵と、複写禁止に変更した複写属性情報を記録装置へ転送する。暗号鍵媒介装置内に保管している複写属性情報も、複写禁止に変更する。ステップ3017は、記録装置が暗号鍵を独自に暗号化して記録する。ステップ3018は、記録装置に暗号化した番組と複写禁止の複写属性情報を記録する。

【0125】ステップ3019は、複写回数が1回に制限されていない場合で、暗号鍵媒介装置の認証を行う。ステップ3020は、暗号鍵媒介装置へ暗号鍵と複写許可の複写属性情報を転送する。ステップ3021は、暗号鍵媒介装置と記録装置の間で認証を行う。ステップ3022は、暗号鍵媒介装置から暗号鍵と、複写許可の複写属性情報を記録装置へ転送する。ステップ3023は、記録装置が暗号鍵を独自に暗号化して記録する。ステップ3024は、記録装置に暗号化した番組と複写許可の複写属性情報を記録する。

【0126】ステップ3010へ分岐した後は、ステップ3025で、出力先がPCなどのコンピュータかどうかを判定し、コンピュータでもない場合は、終了する。(他に出力先として使用できる機器がある場合には、さらに分岐して、処理を行う)ステップ3026は、出力先がコンピュータの場合で、選択した番組が複写制限なしかどうかを判定し、複写制限がある場合には、終了してコンピュータに対しては、何も出力しない。ステップ3027は、複写制限が無い場合で、暗号鍵媒介装置を認証する。ステップ3028は、暗号鍵媒介装置へ暗号

鍵と出力先がコンピュータであるという出力先情報を転送する。ステップ3029は、暗号鍵媒介装置から暗号鍵の識別情報をコンピュータへ転送する。ステップ3030は、コンピュータに暗号化した番組と暗号鍵の識別情報を記録する。

【0127】以上により、記録するのに制限がある場合にも対応して処理を行う。コンピュータには、制限のある番組を記録しないことで、違法なコピーを防ぎ、著作権を保護することができる。

【0128】図33は、暗号鍵媒介装置がリモコンなどを兼用して、提示装置と対になったICカードを装着する形態の場合の処理の流れ図を示す。また、図34は、受信機と暗号鍵媒介装置、ICカード、提示装置の間の処理シーケンスを示す。対応する処理に図33と同じ番号が付されている。

【0129】ステップ3301は、提示装置と対になったICカードを暗号鍵媒介装置へ装着する。ステップ3302は、暗号鍵媒介装置とICカードが認証処理を行う。ステップ3303は、視聴あるいは記録する番組を選択する。ステップ3304は、暗号鍵媒介装置が送信側機器を認証する。ステップ3305は、暗号鍵を送信側機器と暗号鍵媒介装置の間の専用の暗号化処理を行って、暗号鍵媒介装置へ転送する。

【0130】ステップ3306は、暗号鍵媒介装置が暗号鍵の暗号を解除する。ステップ3307は、解除した暗号鍵をICカードの識別情報を元にした共通鍵で暗号化を施す。ステップ3308は、ICカードへ暗号化した暗号鍵を転送する。ステップ3309は、暗号鍵媒介装置と受信側機器がICカードの識別情報などを使用して認証処理を行う。ステップ3310は、暗号化した暗号鍵を使用するときに、ICカードから暗号鍵媒介装置へ転送する。ステップ3311は、暗号鍵媒介装置から、暗号化した暗号鍵を受信側機器へ転送する。ステップ3312は、受信側機器が提示装置の場合で、暗号化した暗号鍵を共通鍵で解除して、番組を再生提示する。ステップ3313は、受信側機器が記録装置の場合で、暗号化した暗号鍵をそのまま記録する。

【0131】また、図23、図24の例と同様に、送信側機器から受信側機器へ暗号鍵媒介装置とICカードの識別情報を送信して、暗号鍵媒介装置と受信側機器の認証に使用する方法も可能である。

【0132】以上により、送信側機器から暗号鍵媒介装置への暗号鍵の転送は、機器ごとに独自の仕様で暗号化を行い、暗号鍵媒介装置から、受信側機器への暗号鍵の転送は、ICカードの識別情報を使用した提示装置ごとの共通鍵で暗号化する構成となり、暗号鍵の盗用を困難にすることができる。

【0133】図35は、暗号鍵媒介装置に使用する機器を登録する場合の処理の流れ図を示す。また、図36は、受信機と暗号鍵媒介装置、ICカード、提示装置の

間の処理シーケンスを示す。対応する処理に図35と同じ番号が付されている。

【0134】ステップ3501は、使用する機器を暗号鍵媒介装置へ登録する。ステップ3502は、使用する機器を選択する。ステップ3503は、視聴または記録する番組を選択する。ステップ3504は、送信側機器が、選択した番組を暗号化する暗号鍵を暗号鍵媒介装置への登録情報に基づく共通鍵で暗号化する。ステップ3505は、暗号化した暗号鍵を暗号鍵媒介装置へ転送する。ステップ3506は、暗号鍵媒介装置が、送信側機器の登録情報に基づく共通鍵で暗号鍵の暗号を解除する。ステップ3507は、解除した暗号鍵をICカードへ転送する。ステップ3508は、視聴時刻にICカードから暗号鍵を暗号鍵媒介装置へ転送する。

【0135】ステップ3509は、暗号鍵を受信側機器の登録情報に基づく共通鍵で暗号化する。ステップ3510は、暗号鍵媒介装置と受信側機器がICカードの識別情報などを使用して認証処理を行う。ステップ3511は、暗号化した暗号鍵を暗号鍵媒介装置から受信側機器へ転送する。ステップ3512は、受信側機器が提示装置の場合で、暗号鍵の暗号を解除して、番組の暗号を解除して再生提示する。ステップ3513は、受信側機器が記録装置の場合で、暗号化した暗号鍵をそのまま記録する。

【0136】以上により、あらかじめ登録した正規の機器と暗号鍵媒介装置との間では、共通鍵を生成して暗号鍵の受け渡しが行えるが、それ以外の機器との間では、暗号鍵の受け渡しが行えないため、違法な機器での視聴を防ぐことができる。

【0137】図37は、暗号鍵媒介装置がリモコンなどを兼用して、提示装置と対になったICカードを装着する形態の場合の処理の流れ図を示す。また、図38は、受信機と暗号鍵媒介装置、ICカード、提示装置の間の処理シーケンスを示す。対応する処理に図37と同じ番号が付されている。

【0138】ステップ3701は、提示装置と対になったICカードを暗号鍵媒介装置へ装着する。ステップ3702は、暗号鍵媒介装置とICカードが認証処理を行う。ステップ3703は、視聴あるいは記録する番組を選択する。ステップ3704は、暗号鍵媒介装置が送信側機器を認証する。ステップ3705は、暗号鍵を送信側機器と暗号鍵媒介装置の間の専用の暗号化処理を行って、暗号鍵媒介装置へ転送する。

【0139】ステップ3706は、暗号鍵媒介装置が暗号鍵の暗号を解除する。ステップ3707は、解除した暗号鍵をICカードへ転送する。ステップ3708は、ICカードが暗号鍵を暗号化する。ステップ3709は、暗号鍵媒介装置と受信側機器が認証処理を行う。ステップ3710は、ICカードが暗号化した暗号鍵を暗号鍵媒介装置へ転送する。ステップ3711は、暗号鍵

媒介装置が暗号化した暗号鍵を受信側機器へ転送する。ステップ3712は、受信側機器が提示装置の場合で、暗号化した暗号鍵を解除して、番組を再生提示する。ステップ3713は、受信側機器が記録装置の場合で、暗号化した暗号鍵をそのまま記録する。

【0140】以上により、送信側機器から暗号鍵媒体装置への暗号鍵の転送は、機器ごとに独自の仕方で暗号化を行い、暗号鍵媒体装置から、受信側機器への暗号鍵の転送には、ICカードによる提示装置独自の暗号化を用いる構成となり、暗号鍵の盗用を困難にすることができる。

【0141】図39は、提示装置に入力装置、または入力装置の接続部が備えられている場合の処理の流れ図を示す。また、図40は、受信機と暗号鍵媒体装置、提示装置、記録手段の間の処理シーケンスを示す。対応する処理に図39と同じ番号が付されている。

【0142】ステップ3901は、提示装置上で、使用する機器の選択を行う。ステップ3902は、提示装置と選択した使用機器の間で認証を行う。ステップ3903は、選択した送信側機器から番組情報リストを提示装置へ転送する。ステップ3904は、視聴あるいは記録する番組を選択する。

【0143】ステップ3905は、提示装置から番組選択情報を暗号化して、選択した送信側機器へ転送する。ステップ3906は、送信側機器から暗号化した暗号鍵を暗号鍵媒体手段へ電波などで転送する。ステップ3907は、暗号鍵媒体装置が暗号化した暗号鍵を解除する。ステップ3908は、暗号鍵媒体装置が暗号鍵を暗号化して提示装置へ転送する。ステップ3909は、提示装置が暗号鍵の暗号を解除して、番組を再生する。

【0144】ステップ3910は、記録する場合に、提示装置が解除した暗号鍵を暗号化して記録装置へ転送する。ステップ3911は、記録装置が暗号化した暗号鍵をそのまま記録する。

【0145】以上により、暗号鍵媒体装置への情報の入力は、送信側機器からのみとなり、暗号鍵媒体装置からの出力は、提示装置へだけとなり、インターフェースが単純になる。

【0146】図41は、自己録再の番組あるいは、著作権保護に関する制限が無いまたは、編集を許可された番組がある場合の処理の流れ図を示す。

【0147】ステップ4101は、視聴または、記録、編集する番組を選択する。ステップ4102は、自己録再の番組かどうかを判定する。ステップ4103は、自作の番組ではない場合で、著作権保護に関する制限がないかどうかを判定する。ステップ4104は、著作権保護に関する制限がある場合で、編集が許可されているかどうかを判定する。

【0148】ステップ4105は、自己録再の番組または、著作権保護に関する制限がない場合または、編集が

許可されている場合で、暗号化しないで、番組を出力する。ステップ4106は、暗号化されていない番組を提示手段が提示する。あるいは、記録手段などで、記録、編集を行う。

【0149】ステップ4107は、編集が許可されていない場合で、選択した番組を暗号化して出力する。ステップ4108は、提示手段で暗号を解除して提示、または、記録が許可されている時には記録手段で記録する。ステップ4107、4108の具体的な処理は、図30のステップ3003以降の処理になる。

【0150】以上により、著作権保護に関する制限が無いコンテンツなどは、自由に編集作業を行うことができる。

【0151】本発明の実施の形態では、MPEGのコンテンツを暗号化してディスプレイやスピーカへ出力し、ディスプレイ、スピーカで暗号を解除し、MPEGデコードして直接再生するといったことを行うため、暗号化を解除された状態では機器の外部には出力されない。また、暗号鍵も別に暗号化して、コンテンツとは別の系統で送受信し、送信側機器と暗号鍵媒体装置と受信側機器の3者で正常に認証を行った場合にのみ暗号鍵が受信側の機器に渡るため、違法にコピーされても再生することが非常に困難になる。

【0152】

【発明の効果】本発明によれば、著作権を保護しながら視聴者の使い勝手を考慮した新しい暗号化デジタル情報と暗号鍵の伝送装置およびデジタルメディア機器ならびに暗号鍵媒体装置を提供することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態の構成のブロック図を示す。

【図2】図1の受信機101の実施の形態の構成のブロック図を示す。

【図3】図1の提示装置105の第1の実施の形態の構成のブロック図を示す。

【図4】図1の記録装置102の第1の実施の形態の構成のブロック図を示す。

【図5】図1の再生装置103の第1の実施の形態の構成のブロック図を示す。

【図6】図1のコンピュータ103の第1の実施の形態の構成のブロック図を示す。

【図7】図1の提示装置105の第2の実施の形態の構成のブロック図を示す。

【図8】暗号鍵媒体装置の第1の実施の形態の構成のブロック図を示す。

【図9】暗号鍵媒体装置の第2の実施の形態の構成のブロック図を示す。

【図10】暗号鍵媒体装置の第3の実施の形態の構成のブロック図を示す。

【図11】暗号鍵媒体装置の第4の実施の形態の構成の

ブロック図を示す。

【図 12】図 11 の認証手段 1102 の構成のブロック図を示す。

【図 13】暗号鍵媒体装置と第 1 のデジタルメディア機器、第 2 のデジタルメディア機器の認証手段の第 1 の実施の形態の構成のブロック図を示す。

【図 14】暗号鍵媒体装置と第 1 のデジタルメディア機器、第 2 のデジタルメディア機器の第 2 の実施の形態の構成のブロック図を示す。

【図 15】暗号鍵媒体装置と第 1 のデジタルメディア機器、第 2 のデジタルメディア機器の第 3 の実施の形態の構成のブロック図を示す。

【図 16】暗号鍵媒体装置と第 1 のデジタルメディア機器、第 2 のデジタルメディア機器の認証手段の第 4 実施の形態の構成のブロック図を示す。

【図 17】暗号鍵媒体装置の他の構成を示す図である。

【図 18】暗号鍵媒体装置の別の実施の形態の構成のブロック図を示す。

【図 19】暗号鍵媒体装置のさらに別の実施の形態の構成のブロック図を示す。

【図 20】暗号鍵媒体装置のさらに別の実施の形態の構成のブロック図を示す。

【図 21】機器を認証して暗号鍵を転送する処理の流れ図を示す。

【図 22】図 21 の処理シーケンスを示す図である。

【図 23】暗号鍵媒体装置と機器の認証処理だけの流れ図を示す。

【図 24】図 23 の処理シーケンスを示す図である。

【図 25】暗号鍵を送信側機器から受信側機器へ転送する処理だけの流れ図を示す。

【図 26】図 25 の処理シーケンスを示す図である。

【図 27】暗号鍵媒体装置として、送信側機器と受信側機器を直接接続する形態をとる場合の認証と暗号鍵の転送処理の流れ図を示す。

【図 28】PC などのコンピュータへ出力する場合の処理の流れ図を示す。

【図 29】PC などのコンピュータが送信側機器になった場合に視座する処理の流れ図を示す。

【図 30】記録に制限がある場合を含めた処理の流れ図を示す。

【図 31】記録に制限がある場合を含めた処理の流れ図を示す。

【図 32】記録に制限がある場合を含めた処理の流れ図を示す。

【図 33】暗号鍵媒体装置がリモコンなどを兼用して、

IC カードを装着する形態の場合の処理の流れ図を示す。

【図 34】図 33 の処理シーケンスを示す図である。

【図 35】暗号鍵媒体装置に使用する機器を登録する場合の処理の流れ図を示す。

【図 36】図 35 の処理シーケンスを示す図である。

【図 37】暗号鍵媒体装置がリモコンなどを兼用して、IC カードを装着する形態の場合の処理の流れ図を示す。

【図 38】図 37 の処理シーケンスを示す図である。

【図 39】提示装置に入力装置、または入力装置の接続部が備えられている場合の処理の流れ図を示す。

【図 40】図 39 の処理シーケンスを示す図である。

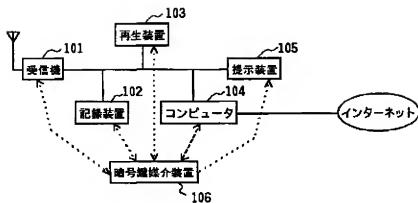
【図 41】著作権保護に関する制限がある場合と無い場合を含めた処理の流れ図を示す。

【符号の説明】

101…受信機、102…記録装置、103…再生装置、104…コンピュータ、105…提示装置、106…暗号鍵媒体装置、201…復調手段、202…誤り訂正手段、203…デスクランブル手段、204…分離手段、205、503…暗号化手段、206、301、401、501、601、1102…認証手段、207、502、1101…暗号鍵生成手段、302…暗号解除手段、303…復号手段、304…映像再生手段、305…音声再生手段、402…暗号鍵用暗号鍵生成手段、403…暗号鍵暗号化復号化手段、404…記録装置、504…記録媒体、602…演算装置、603…記憶装置、604…映像音声変換装置、701…入力先判定手段、702…入力手段、801…暗号鍵熱変換手段、802…熱暗号鍵検出手段、901…暗号鍵振動変換手段、902…振動暗号鍵検出手段、1001…暗号鍵磁界変換手段、1002…抵抗暗号鍵検出手段、1103…乱数発生手段、1104…記憶手段、1105…暗号化復号化手段、1201…提示手段、1202…認識手段、1203…変換手段、1204…処理部、1301…認証部、1302…揮発性光学メモリ、1303…シッター部、1304…受光部、1305…発光部、1306、1403、1502、1602…暗号鍵変換部、1401…記録部、1402…温度感応発生部、1501…圧力感応発生部、1601…超音波発生受信部、1701…可動導体、1702…接点、1801…IC カード、1802…IC カード認証手段、1803…暗号化復号化手段、1804…機器認証手段、1805…電磁波送受信手段、1901…機器登録手段、2001…暗号化 IC カード、2002…暗号鍵復号手段。

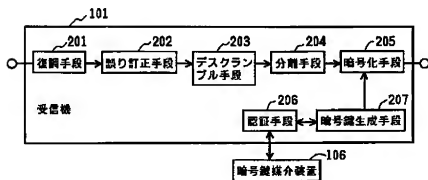
【図1】

図 1



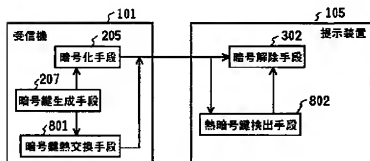
【図2】

図 2



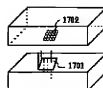
【図8】

図 8



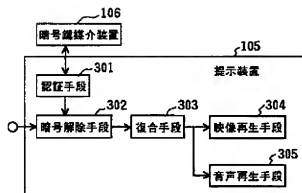
【図17】

図 17



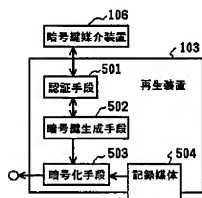
【図3】

図 3



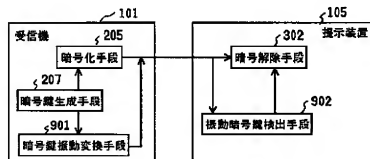
【図5】

図 5



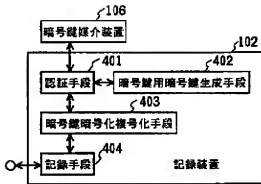
【図9】

図 9



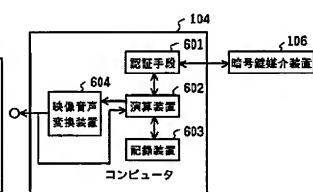
【図4】

図 4



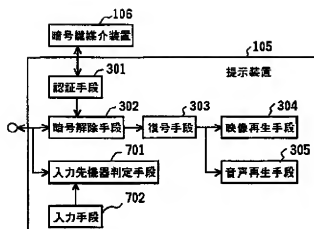
【図6】

図 6



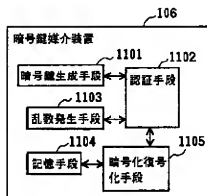
【図7】

図 7



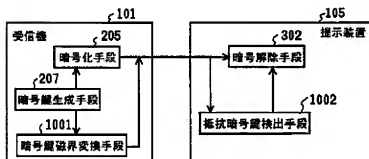
【図11】

図 11



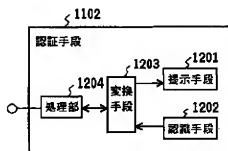
【図10】

図 10



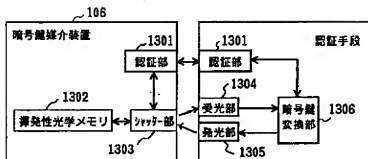
【図12】

図 12



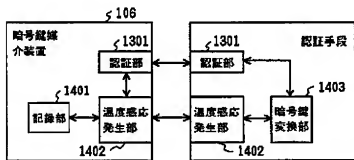
【図13】

図 13



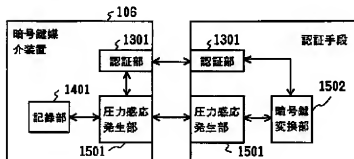
【図14】

図 14



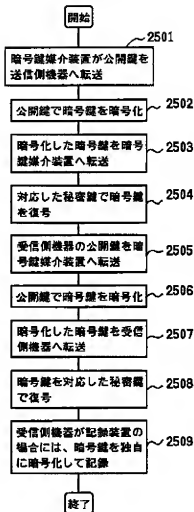
【図15】

図 15



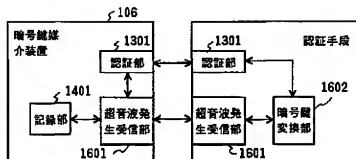
【図25】

図 25



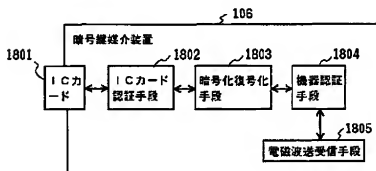
〔図16〕

図 16



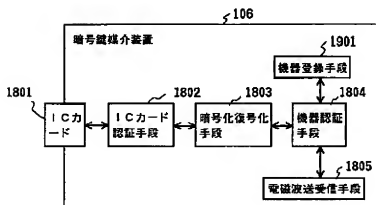
〔図18〕

図 18



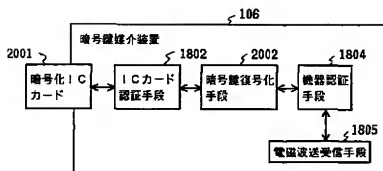
〔図19〕

図 19



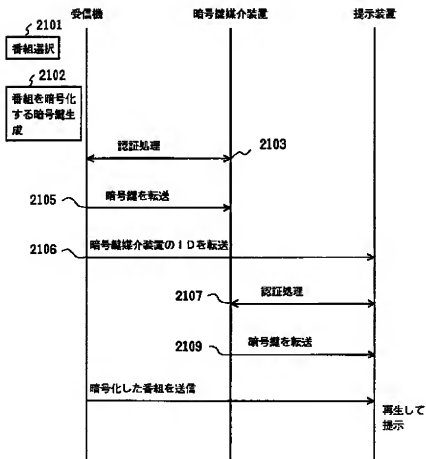
【図20】

図 20

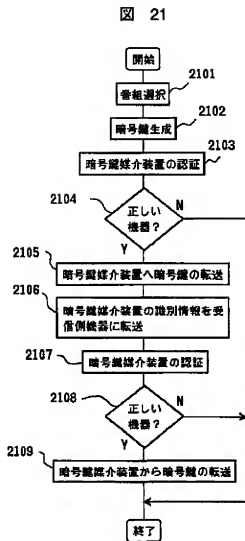


【図22】

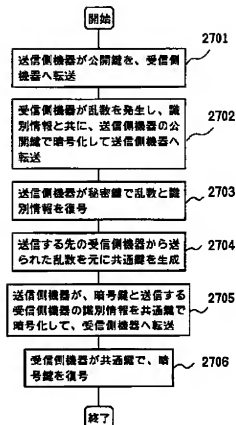
図 22



【図 21】

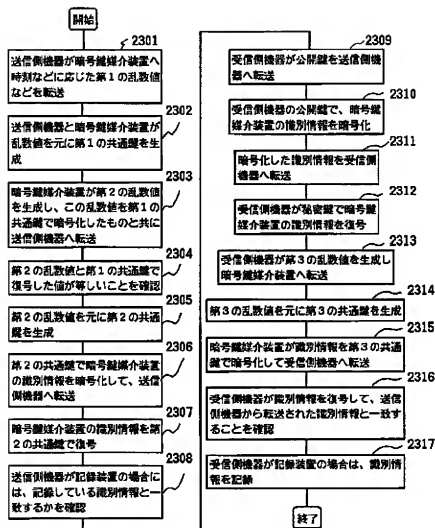


【図 27】



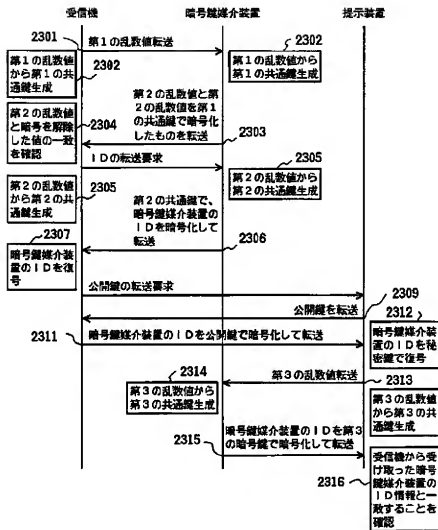
【図23】

図 23



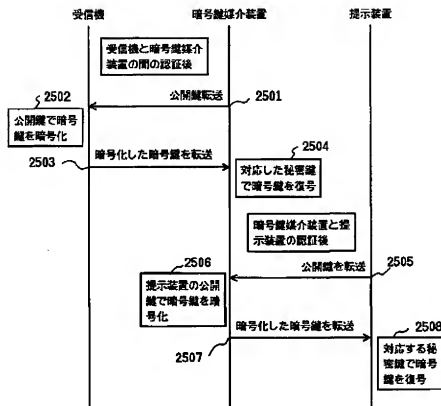
〔図24〕

図 24



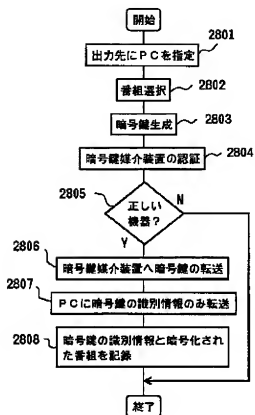
【図26】

図 26



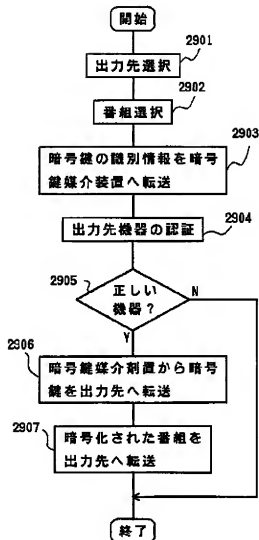
【図28】

図 28



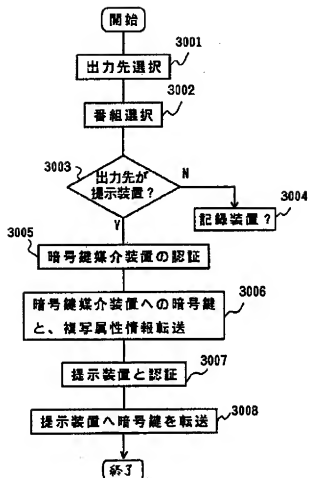
【図29】

図 29



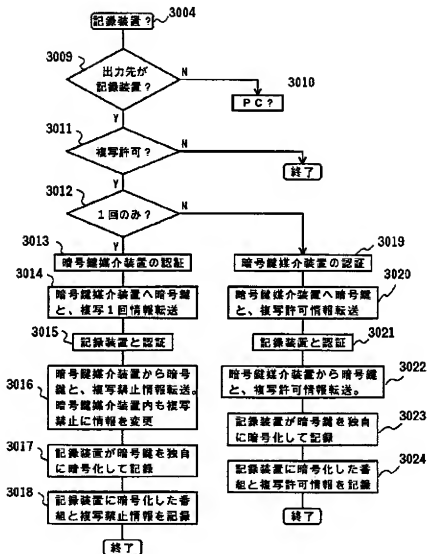
【図30】

図 30



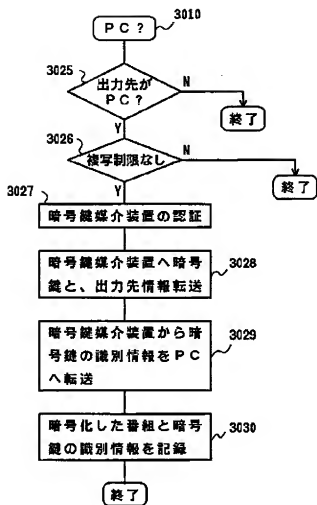
【図31】

図 31



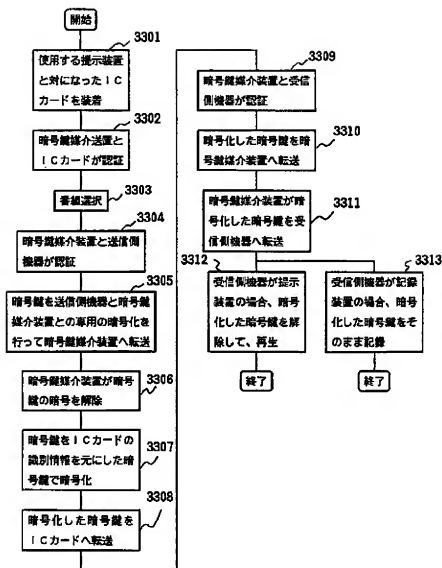
【図32】

図 32



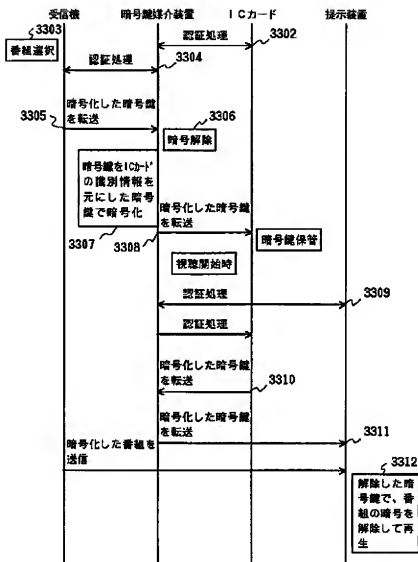
【図 33】

図 33



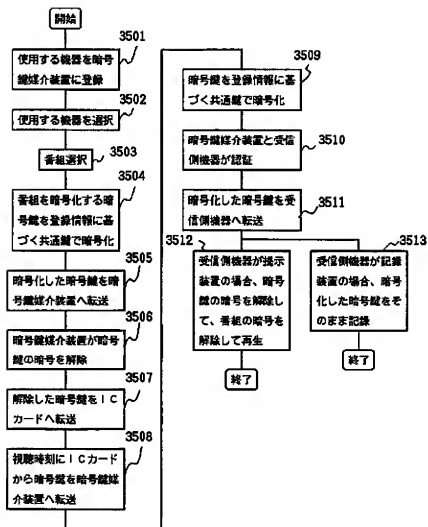
【図34】

図 34



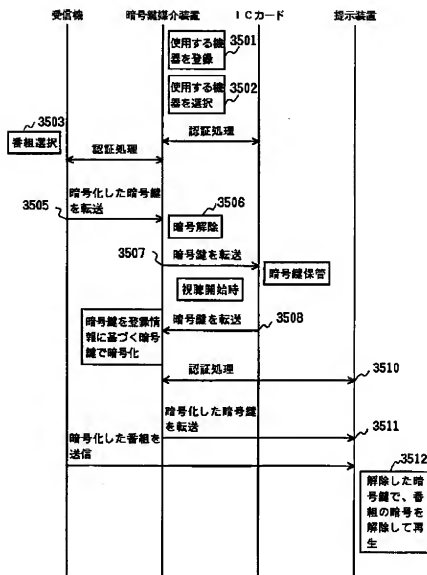
【図 35】

図 35



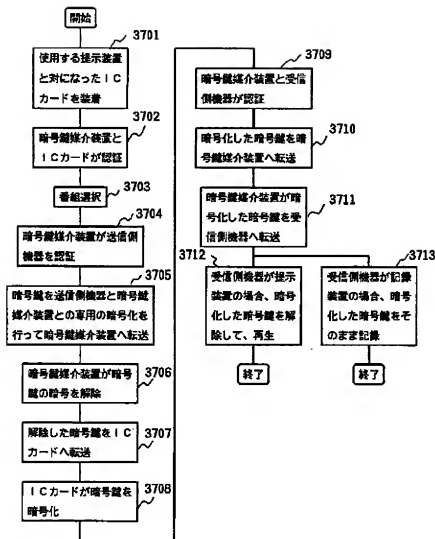
【図36】

図 36



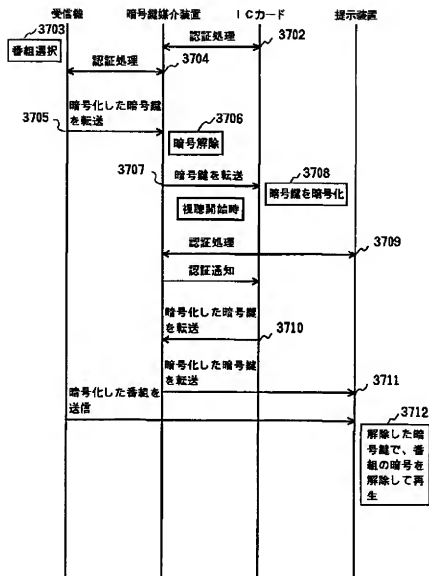
【図37】

図 37



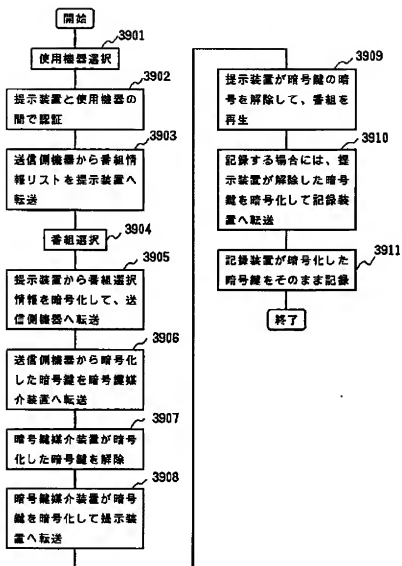
【図38】

図 38



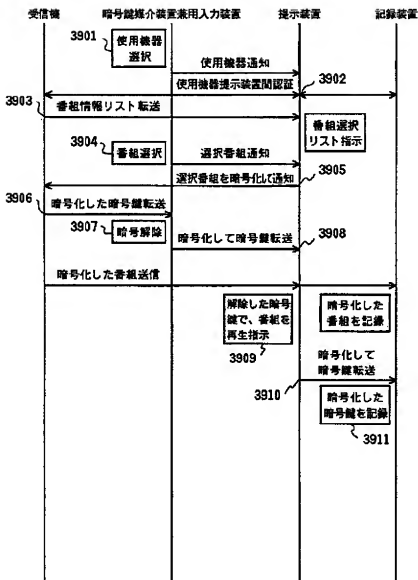
【図39】

図 39



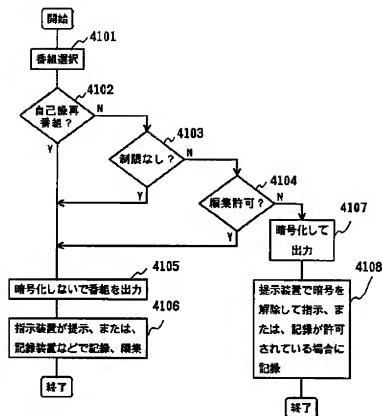
【図 40】

図 40



【図41】

図 41



フロントページの続き

(51)Int. Cl.⁷

識別記号

F I

H 0 4 N 7/167

キーワード(参考)

Z

(72)発明者 高清水 聡
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内
(72)発明者 米田 茂
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内
(72)発明者 根本 敏之
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

(72)発明者 鶴賀 貞雄
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内
(72)発明者 是枝 浩行
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内
(72)発明者 岡村 巧
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

F ターム(参考) 58017 AA03 BA07 BB09
58035 AA13 BB09 BC03 CA38
5C053 FA13 FA21 FA25 GB37 JA30
5C064 CA14 CB01 CC04
5J104 AA13 AA15 AA16 EA06 EA19
NA02 NA35 NA37 PA05